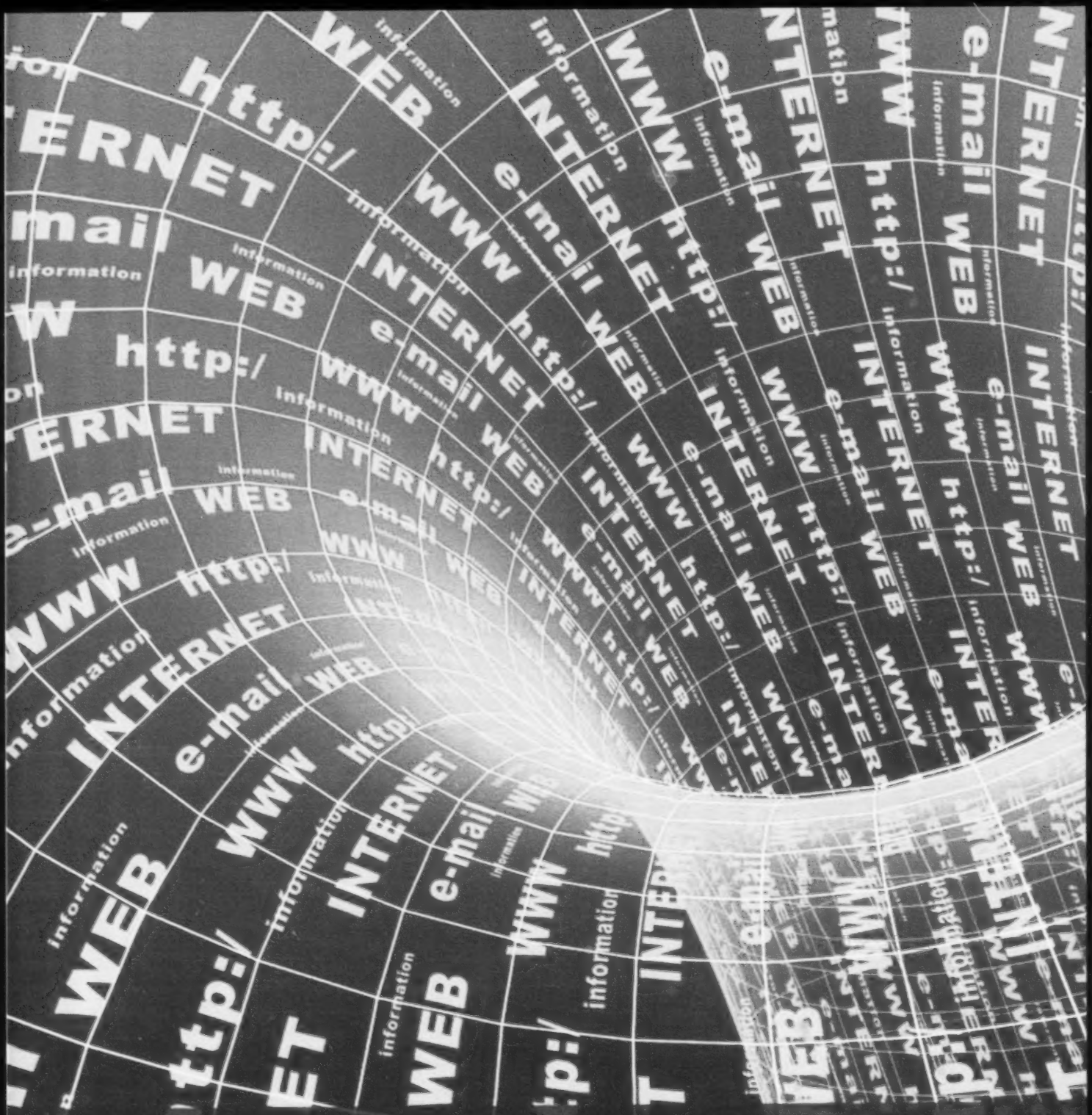


2011 ACCÈS À L'INFORMATION ET VIE PRIVÉE

TOUJOURS VIGILANTS

Information and Privacy
Commissioner/Ontario
Commissaire à l'information
et à la protection de la vie privée/Ontario

Le 4 juin 2012

L'honorable Dave Levac
Président de l'Assemblée législative de l'Ontario

Monsieur le Président,

J'ai l'honneur de présenter à l'Assemblée législative le rapport annuel 2011 du Commissaire à l'information et à la protection de la vie privée de l'Ontario.

Ce rapport porte sur la période allant du 1er janvier au 31 décembre 2011.

Veuillez prendre note que des renseignements supplémentaires sur nos activités de 2011, notamment tout l'éventail de statistiques, d'analyses et de documents à l'appui, se trouvent dans la section de notre rapport annuel en ligne à www.ipc.on.ca.

Veuillez agréer, Monsieur le Président, l'assurance de ma haute considération.

La commissaire,

Ann Cavoukian, Ph.D.

p.j.

2 Bloor Street East
Suite 1400
Toronto, Ontario
M4W 1A8

2, rue Bloor est
Bureau 1400
Toronto (Ontario)
M4W 1A8

416-326-3333
1-800-387-0073
Fax/Téléc: 416-325-9195
TTY: 416-325-7539
http://www.ipc.on.ca

MESSAGE DE LA COMMISSAIRE

Ann Cavoukian, Ph.D.
Commissaire à l'information et
à la protection de la vie privée,
Ontario, Canada

Le début de 2011 s'annonçait très prometteur, grâce aux progrès réalisés sur le plan de l'accès à l'information et de la protection de la vie privée. Cependant, à la fin de l'année, je me suis retrouvée à nouveau contrainte (comme à maintes reprises par le passé) de mobiliser mes ressources pour me lancer à la défense de la vie privée. C'est pourquoi, pour le rapport annuel de cette année, j'ai choisi le thème ***Toujours vigilants***.

La *protection intégrée de la vie privée* continue de connaître un essor fulgurant à l'échelle mondiale – elle est reconnue comme la norme internationale de protection de la vie privée et a été traduite en 25 langues. Toutefois, ici même au Canada a surgi une véritable menace à la vie privée.

Le nouveau dépôt prévu d'un projet de loi sur ce que l'on appelle l'« accès légal », en remplacement des projets de loi morts au Feuilleton lors du déclenchement des élections fédérales en mars, a retenu mon attention l'automne dernier (au moment où le présent rapport annuel a été rédigé, ce nouveau texte de loi, le projet de loi C-30, a été déposé au Parlement). Mon bureau a lancé rapidement une campagne d'information pour sensibiliser la population aux sérieuses inquiétudes en matière de vie privée que j'entretenais au sujet de ce projet de loi dont l'adoption, à mon avis, entraînerait tout simplement la création d'un régime de surveillance sanctionné par l'État.

En ce qui concerne l'accès à l'information, nous avons connu une autre année productive. J'ai passé une bonne partie de 2011 à consulter des dirigeants d'hôpitaux de l'Ontario et à collaborer avec eux pour les aider à se préparer à l'application de la *Loi sur l'accès à l'information et la protection de la vie privée* (*LAIPVP*), que je réclamais depuis de longues années. Je leur ai conseillé d'envisager la divulgation de renseignements selon une démarche proactive et non réactive, c'est-à-dire d'établir un processus automatique de divulgation de renseignements.

En outre, le concept de plus en plus répandu des « données ouvertes » m'a beaucoup encouragée. Je suis très favorable à ce concept, selon lequel certains types de documents généraux ne contenant pas de renseignements personnels sont mis à la disposition de quiconque veut les utiliser et les reproduire, sans restriction.

Dans l'ensemble, 2011 a été une année équilibrée, où nous avons connu des hauts et des bas, une année de grandes réussites mais aussi de lourds défis.

Accès légal

Au début de l'année, j'étais ravie des progrès réalisés du côté de la promotion du concept de *protection intégrée de la vie privée* (*PIVP*) dans le monde. On m'a même dit à plusieurs reprises que la *PIVP* était sur toutes les lèvres. Ce succès m'a convaincue qu'il est vraiment possible d'assurer la protection de la vie privée à une époque où la connectivité s'intensifie. C'est pourquoi j'ai été vraiment étonnée de découvrir, au milieu de l'année, que surgissait dans notre propre pays l'une des menaces les plus sérieuses à la vie privée.

Pendant les élections fédérales, le gouvernement a promis de déposer à nouveau un projet de loi sur l'accès légal advenant qu'il soit réélu. Si ce texte de loi était adopté sous sa forme actuelle, la police serait autorisée à accéder aux données sur les abonnés sans mandat ni surveillance judiciaire, ce qui soulève des inquiétudes dans une société libre et démocratique.

J'ai été troublée d'entendre l'honorable Vic Toews, ministre fédéral de la Sécurité publique, affirmer que les renseignements personnels en question revenaient simplement à ceux que l'on peut trouver dans un « annuaire téléphonique ». Or, il n'y a rien de plus faux! Cette affirmation m'a poussée à écrire une lettre ouverte au ministre. J'ai également informé le public en rédigeant deux articles d'opinion pour le *National Post* et en continuant d'échanger avec le ministre dans une série de lettres qui ont paru dans le courrier des

lecteurs, où nous avons exposé avec respect nos points de vue divergents.

Mon message au ministre et aux personnes partageant son point de vue était que les renseignements en question ne sont *pas du tout* les mêmes que ceux que l'on trouve dans un annuaire téléphonique. Les données sur les abonnés de services d'accès à Internet, qui comprennent six champs (adresse IP, adresse électronique et quatre autres champs de renseignements personnels) sont bien plus détaillées que le contenu d'un annuaire, surtout quand on tient compte des données qui peuvent être associées à ces éléments d'information. De nouveaux outils analytiques et algorithmes permettent désormais non seulement d'associer un numéro comme une adresse IP à un particulier pouvant être identifié, mais aussi de combiner des renseignements émanant de sources multiples, afin de créer en bout de ligne un portrait détaillé de ce particulier.

Défi de la *protection intégrée de la vie privée* (2011)

La *protection intégrée de la vie privée* en 2011

En 2011, plus d'organismes que jamais ont adopté les principes de la *PIVP*, ce qui a permis de chasser le mythe courant selon lequel la protection de la vie privée se fait au prix de l'innovation. C'est faux et c'est même le contraire : pour obtenir un système tout à fait fonctionnel qui assure une excellente protection de la vie privée, il faut faire preuve d'une innovation inégalée. En tant que spécialiste de la vie privée, je crois que l'intégration de la protection de la vie privée comme exigence de base est en voie de devenir une grande tendance de notre époque, à juste titre.

La *protection intégrée de la vie privée a posteriori*

En 2011 est née une première notion dérivée de la *protection intégrée de la vie privée*, la *protection intégrée de la vie privée a posteriori* (*PIVPP*), qui procure un cadre pour le renforcement de la protection de la vie privée dans les systèmes déjà établis, auxquels des caractéristiques de protection de la vie privée n'avaient pu être intégrées au moment de leur conception. Présentée dans un livre blanc rédigé en collaboration avec Marilyn Prosch, *Privacy by ReDesign: Building a Better Legacy*, la *PIVPP* est un processus transformateur qui encadre l'évaluation proactive des lacunes des systèmes existants et définit comment il est possible de les combler systématiquement par une opération à trois volets qui consiste à *repenser, refondre et relancer* ces systèmes.

La *protection intégrée de la vie privée* à l'étranger

La *protection intégrée de la vie privée* a été beaucoup préconisée dans le monde en 2011. Voici quelques progrès remarquables à cet égard.

- L'Union européenne a annoncé le *Cadre d'évaluation de l'impact des applications RFID sur le respect de la vie privée et la protection des données*, un accord marquant qui fait du respect de la vie privée des consommateurs un élément essentiel de l'implantation de la technologie des étiquettes intelligentes fondée sur la *protection intégrée de la vie privée*.
- John Kerry et John McCain, sénateurs américains, ont cité la *protection intégrée de la vie privée* dans leur projet de charte des droits sur la protection de la vie privée dans le secteur privé.
- Le premier défi de réalisations d'applications protégeant la vie privée, *Develop for Privacy Challenge*, organisé par l'American Civil Liberties Union of Northern California and Washington, a encouragé des réalisateurs d'applications mobiles à intégrer la *protection intégrée de la vie privée* de façons novatrices pour permettre aux usagers de gérer leurs renseignements personnels.

Séance d'information sur le processus de transformation à la base de la *protection intégrée de la vie privée a posteriori* (Mexico), 1er novembre 2011 : Peter Hustinx, contrôleur européen de la protection des données; Mary Ellen Callahan, chef de la protection de la vie privée, département de la Sécurité intérieure des États-Unis; Ann Cavoukian, Ph.D., commissaire à l'information et à la protection de la vie privée de l'Ontario; Tom Marinelli, vice-président directeur et directeur général de l'information, Société des loteries et des jeux de l'Ontario; Jules Polonetsky, coprésident et directeur, The Future of Privacy Forum

- La commission des services publics de Californie a reconnu que «...la méthodologie de la *protection intégrée de la vie privée* représente une démarche prometteuse pour faire en sorte que les pratiques relatives aux données favorisent la protection de la vie privée, non seulement pour assurer la minimisation des données comme pratique équitable en matière de renseignements, mais aussi relativement à tous les aspects de la planification de la protection de la vie privée ».
- De nombreux projets conjoints de *PIVP* ont été réalisés en 2011. Mon bureau a annoncé un partenariat avec San Diego Gas & Electric (une filiale de Sempra) pour intégrer la *protection intégrée de la vie privée* dans son régime de prix dynamiques fondé sur l'utilisation de compteurs intelligents, nous avons publié un document conjointement avec le Groupe de travail international sur la protection des données dans les télécommunications de Berlin intitulé *Privacy by Design and Smart Metering: Minimize Personal Information to Maintain Privacy*, et nous avons entrepris la rédaction d'un document s'appuyant sur des études européennes et l'expérience de compagnies d'électricité concernant l'implantation de compteurs intelligents selon les principes de la *PIVP*. Ce document sera publié en 2012.

La *protection intégrée de la vie privée* en Ontario

Mon bureau a également consacré beaucoup d'efforts en 2011 à faire progresser la *PIVP* en Ontario en formant des partenariats pour orienter l'avenir de la protection de la vie privée.

Au début de janvier, j'ai appelé 2011 l'« année de l'ingénieur ». Je tenais alors beaucoup à m'adresser aux personnes qui conçoivent et réalisent les systèmes et technologies dont nous dépendons de plus en plus. J'ai donc passé une bonne partie de l'année à sensibiliser les ingénieurs et réalisateurs à la *PIVP* afin d'en assurer l'adoption dans des dizaines d'entreprises de technologie parmi les plus novatrices au monde.

En février, nous avons publié notre troisième document sur la protection de la vie privée et le réseau électrique intelligent, intitulé *Operationalizing Privacy by Design: The Ontario Smart Grid Case Study*, qui propose des exemples de la façon dont les services publics et les fournisseurs de biens et services peuvent se servir des pratiques exemplaires sur la *protection intégrée de la vie privée* dans les réseaux électriques intelligents aux fins de la mise en œuvre de tels réseaux.

En mai, la Société des loteries et des jeux de l'Ontario (OLG) a mis en œuvre son programme de reconnaissance faciale tant attendu dans ses 27 établissements de jeu de l'Ontario. Je suis fière d'avoir contribué un peu à la création de ce système, en collaboration avec le professeur Kostas Plataniotis et Karl Martin, Ph.D., chercheurs à l'Université de Toronto, car elle assure une protection bien supérieure de la vie privée que la simple reconnaissance faciale, sans pour autant réduire les fonctionnalités, la sécurité ou le rendement. Il s'agit donc d'un exemple bien concret d'application de la *protection intégrée de la vie privée*.

En juin, nous avons publié un livre blanc conjointement avec Kim Cameron, expert renommé dans le domaine de l'identité numérique, intitulé *Wi-Fi Positioning Systems: Beware of Unintended Consequences – Issues Involving the Unforeseen Uses of Pre-existing Architecture*. Dans ce document, nous examinons les conséquences involontaires sur la vie privée de la géolocalisation des personnes au moyen de leurs appareils mobiles.

En septembre, nous avons publié un livre blanc rédigé conjointement avec IBM, *Privacy by Design: From Policy to Practice*, qui examine comment cette entreprise a intégré la *protection intégrée de la vie privée* dans ses activités et apporté à ses procédés des améliorations qui ont permis de réduire les frais d'exploitation et de mettre sur pied un processus de conformité bien documenté.

En septembre également, nous avons envisagé la *PIVP* dans le contexte de la réglementation, en publiant le livre blanc intitulé *Privacy by Design in Law, Policy and Practice: A White Paper for Regulators, Decision-makers and Policy-makers*, qui propose l'intégration de la *PIVP* dans les politiques, lois et pratiques.

Nous avons fait beaucoup de progrès cette année sur le plan de la *PIVP*, mais il reste beaucoup à faire. Mon bureau demeure résolu à assurer une meilleure compréhension de l'application de la *protection intégrée de la vie privée* au pays et à l'étranger.

Les hôpitaux désormais assujettis à la *LAIPVP*

À la fin de 2010, lorsque la *Loi de 2010 sur la responsabilisation du secteur parapublic* reçut la sanction royale, j'étais ravie que l'Ontario se joigne enfin aux autres provinces en assujettissant ses hôpitaux à ses lois sur l'accès à l'information.

Cette loi ne devait s'appliquer aux hôpitaux qu'à compter du 1er janvier 2012, mais j'ai profité de ce délai, en 2011, pour aider les hôpitaux à se préparer à ce nouveau régime législatif. L'une des premières mesures que j'ai prises à cet égard a été la publication de deux documents, *Application de la LPRPS et de la LAIPVP aux renseignements personnels sur la santé : Directives à l'intention des hôpitaux*, et *Les hôpitaux et l'accès à l'information : questions fréquentes*.

En outre, j'ai passé une bonne partie de l'année à faire des exposés et à rencontrer le conseil d'administration de différents hôpitaux pour les sensibiliser à la nouvelle loi. Surtout, je voulais calmer leur crainte éventuelle que les lois sur l'accès à l'information ne nuisent au fonctionnement normal des hôpitaux ou à la prestation des soins de santé.

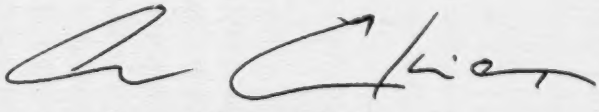
Données ouvertes

Pour la première fois de son histoire, le CIPVP greffera des statistiques brutes à la version de son rapport annuel accessible en ligne. Les universitaires, chercheurs, décideurs et membres du public auront donc accès à des données portant notamment sur les *demandes d'accès à l'information* et sur le *respect du délai de réponse*. Ces données peuvent être comparées à celles de certaines institutions publiques et à d'autres variables, permettant ainsi de mener des recherches très approfondies. Ce nouveau projet m'enthousiasme beaucoup car il rapproche mon bureau de l'idéal de l'accès à l'information.

Semaine du droit à l'information 2011 (Hôpital Mount Sinai) : Joseph Mapa, directeur général, Hôpital Mount Sinai; Rob Devitt, directeur général, Toronto East General Hospital; Ann Cavoukian, Ph.D., commissaire à l'information et à la protection de la vie privée de l'Ontario, Canada; Tom Closson, président-directeur général de l'Association des hôpitaux de l'Ontario

Remerciements

Comme toujours, je tiens à remercier chaleureusement l'ensemble de mon personnel. Son dévouement et son travail soutenu ont fait de notre bureau un organisme de premier plan, dont les travaux sont maintenant connus dans le monde entier. Notre réussite repose sur la passion et l'enthousiasme de l'équipe avec laquelle j'ai l'honneur de collaborer. Je crois vraiment que les Ontariennes et Ontariens ont beaucoup de chance d'avoir à leur service des professionnels aussi talentueux. Je ne pourrais avoir une meilleure équipe, et j'en suis vraiment ravie! Encore et toujours, merci.



Ann Cavoukian, Ph.D.

Commissaire à l'information et à la protection de la vie privée, Ontario, Canada

TABLE DES MATIÈRES

Lettre au président	DC
Message de la Commissaire	1
Questions clés	6
Accès à l'information 2011	11
La *LPRPS* en 2011	14
Demandes du public	16
Respect du délai de réponse	17
Appels – accès à l'information	18
Plaintes concernant la protection de la vie privée	19
La *Loi sur la protection des renseignements personnels sur la santé (LPRPS)*	20
Révisions judiciaires	22
Perspectives d'avenir	23
État financier	TC

Attention à la « surveillance intégrée » : un projet de loi fédéral menace la liberté et la vie privée

Le choix du thème de mon rapport annuel 2011, *Toujours vigilants*, découle en bonne partie du fait que cette année, les Ontariennes et Ontariens se sont retrouvés devant l'une des menaces à la vie privée et à la liberté les plus graves que j'ai rencontrées dans les 25 ans où j'ai protégé les droits des citoyens et préconisé l'ouverture et la transparence au sein des gouvernements.

Cette menace a été le dépôt par le gouvernement fédéral de projets de loi sur l'accès légal. Ces textes de loi visaient à conférer à la police des pouvoirs considérablement accrus leur permettant de retracer des renseignements sur des particuliers pouvant être identifiés au moyen des technologies de communication que nous employons tous les jours : Internet, téléphones intelligents et autres appareils mobiles, parfois sans mandat ni autorisation judiciaire. Les fournisseurs de services de télécommunication seraient également tenus d'intégrer dans leurs réseaux des fonctions d'interception à l'usage de la police.

À mon avis, il est très trompeur de prétendre que de tels projets de loi portent sur l'« accès légal » ou qu'ils visent à protéger les enfants. Ces pouvoirs élargis représentent beaucoup plus : un régime de *surveillance intégrée*.

Je tiens nos services de police en très haute estime, et j'apprécie beaucoup leur travail essentiel en matière de sécurité publique. Cependant, nous devons faire preuve de vigilance et éviter que les besoins de ces services en matière d'enquête ne portent atteinte au droit « à la protection contre les fouilles, les perquisitions ou les saisies abusives » protégé par la constitution.

Faute de modifications considérables, ces projets de loi porteraient atteinte à la vie privée d'un trop grand nombre de personnes innocentes. La surveillance électronique permet de tracer un portrait détaillé et révélateur d'une personne, et de recueillir en même temps des renseignements personnels sur sa famille, ses amis, ses voisins, ses collègues et ses connaissances. De tels pouvoirs de surveillance peuvent se révéler inestimables pour les autorités policières dans la mesure où ils font l'objet d'une supervision adéquate. Par contre, sans supervision, l'exercice de tels pouvoirs peut avoir des conséquences dévastatrices pour des personnes innocentes, qui seront injustement soupçonnées, associées à des éléments de preuve recueillis de façon irrégulière ou jugées de façon inconsidérée.

Tous les commissaires à la protection de la vie privée du Canada ont jugé ces projets de loi si troublants qu'ils ont fait parvenir au sous-ministre fédéral de la Sécurité publique, en mars 2011, une lettre conjointe décrivant leurs préoccupations. Nous avons remis cette lettre au Comité permanent de la sécurité publique et nationale et au Comité permanent de la justice et des droits de la personne de la Chambre des communes.

Les projets de loi C-50, C-51 et C-52 sont morts au Feuilleton lorsque le Parlement a été dissous en mars 2011. Cependant, le gouvernement a promis de les redéposer advenant qu'il soit réélu. (Au moment de rédiger le présent rapport annuel, le projet de loi C-30 a été déposé. Des précisions sont fournies à www.realprivacy.ca.)

Comme je disposais d'une excellente occasion de faire connaître mon point de vue au public et au gouvernement avant le dépôt d'un nouveau projet de loi, j'ai décidé d'écrire ma propre lettre ouverte de 22 pages au ministre de la Sécurité publique et au ministre de la Justice et Procureur général du Canada pour leur faire part de mes préoccupations. J'ai également écrit plusieurs articles d'opinion à l'automne 2011. Puis, en décembre 2011, j'ai décidé d'intensifier ma campagne de sensibilisation, en tenant un colloque avec des leaders d'opinion éminents qui devait avoir lieu en janvier 2012 sous le thème *Attention à la « surveillance intégrée » : défendons les libertés et le droit à la vie privée*. J'ai invité la population ontarienne et même tous les Canadiens et Canadiennes à écrire à leur député fédéral pour lui faire part de leurs préoccupations concernant les projets de loi. Enfin, j'ai demandé à mon personnel d'élaborer des recommandations concrètes en vue de modifier le projet de loi pour établir un régime de maintien de l'ordre moderne, efficace et complet dans lequel seraient intégrées des mesures assurant la protection de la vie privée et la transparence du gouvernement.

À la recherche d'ingénieurs en protection de la vie privée

Nous devons trouver de meilleurs moyens de sécuriser Internet, qui s'appuient non pas sur une intervention accrue du gouvernement, mais plutôt sur l'action des entreprises et des utilisateurs eux-mêmes.

Jonathan Zittrain, *article paru dans Scientific American, 2011*

La *protection intégrée de la vie privée* est arrivée à une étape cruciale de son évolution. La démarche et les principes qu'elle comporte sont désormais reconnus dans le monde entier comme étant essentiels pour obtenir les résultats suivants :

- une protection de la vie privée implicite, et non en réaction à des incidents;
- des précautions efficaces de bout en bout;
- la participation accrue des utilisateurs;
- une transparence et une obligation redditionnelle authentiques;
- un leadership proactif en matière de protection de la vie privée;
- des méthodes systématiques et vérifiables;
- des résultats concrets et mesurables.

Reconnus comme une norme internationale par les commissaires internationaux de la vie privée et de la protection des données en octobre 2010, les principes fondamentaux de la *protection intégrée de la vie privée* ont depuis été adoptés par des décideurs, des législateurs, des groupes industriels et des associations, qui se fondent sur eux afin de refondre leurs régimes de gestion de la protection des renseignements personnels pour le XXI[e] siècle.

La prochaine étape de l'évolution de la *protection intégrée de la vie privée* sera de traduire ces principes en exigences, cahiers des charges, normes, pratiques exemplaires et critères de rendement opérationnel. Cette tâche nécessite une aide spécialisée. Le rôle croissant du directeur général de la protection de la vie privée au sein des organisations témoigne de l'importance stratégique de bien gérer l'information et de la demande dont font l'objet ces spécialistes en raison de leurs compétences. La gestion de la protection de la vie privée en tant que discipline distincte est en voie d'être normalisée et professionnalisée, et il y a actuellement une pénurie d'ingénieurs et d'architectes en protection de la vie privée qualifiés.

L'INGÉNIEUR, C'EST VOUS

« Le code fait loi », a écrit Lawrence Lessig dans un célèbre article. Par extension, il a montré qu'il est possible, voire nécessaire, de fonder le cyberespace sur une architecture qui protège nos valeurs fondamentales. Faute d'intégrer ces valeurs dans les plus brefs délais, nous pourrions en subir des conséquences indésirables. La tâche de l'ingénieur de la protection de la vie privée est donc d'intégrer des valeurs et des préférences dans la conception et le fonctionnement des technologies, systèmes et infrastructures de l'information.

Les principes de la *protection intégrée de la vie privée* peuvent contribuer à réaliser cet objectif en favorisant :

- l'établissement d'objectifs clairs en matière de protection de la vie privée;
- l'adoption de méthodologies systématiques et vérifiables;
- des résultats concrets et mesurables;
- l'imagination, la créativité et l'innovation.

Nous voulons aider les ingénieurs de toutes les spécialités à élaborer et à adopter des pratiques exemplaires en matière de protection de la vie privée et à partager leurs expériences en matière de mise en œuvre, et les reconnaître pour les solutions novatrices qu'ils mettent au point.

Telle était mon intention en déclarant l'« année de l'ingénieur »!

C'est pourquoi j'ai décidé de désigner 2011 l'« année de l'ingénieur ». Afin de joindre un éventail plus large d'experts, mon bureau n'a pas ménagé ses efforts en 2011 pour sensibiliser :

- des médias du secteur des technologies;
- des réalisateurs d'applications mobiles;
- des laboratoires et groupes de recherche;
- des entreprises en démarrage et des multinationales;
- des consortiums d'industries;
- des groupes de normalisation;
- des architectes de l'information et de la sécurité;
- des ingénieurs (au sens large du terme).

Le CIPVP a entamé un dialogue avec ces intervenants du monde entier en vue de se fonder sur les sept principes fondamentaux de la *PIVP* pour élaborer des spécifications de projets, des normes d'approvisionnement et des résultats opérationnels à somme positive.

Votre mot de passe, c'est vous

La biométrie, c'est un mot compliqué qui désigne la mesure de caractéristiques corporelles. Plus ces caractéristiques biométriques sont uniques et stables, mieux elles conviennent à la vérification de l'identité d'une personne. Nous avons beaucoup évolué depuis l'époque des signatures et des cartes à empreintes digitales. De nos jours, la biométrie est entièrement numérique; des systèmes informatiques détectent et mesurent des caractéristiques physiques ou comportementales en temps réel et les comparent à des échantillons « de référence » stockés en mémoire, puis remplissent certaines fonctions selon que ces caractéristiques correspondent ou non.

Dans les œuvres de fiction, la biométrie est partout : un agent secret est incapable de pénétrer dans un laboratoire à haute sécurité ennemi parce que l'accès y est autorisé uniquement par balayage de l'iris; un détective compare la photo granuleuse d'un suspect au contenu d'une base de données énorme et obtient une correspondance en quelques secondes; un avocat de la défense renverse la condamnation de son client sur la base d'un échantillon d'ADN en lui trouvant un jumeau identique!

La réalité rattrape ces scénarios de film : en effet, il devient désormais possible d'identifier automatiquement des gens à des endroits et dans des contextes où ils ne veulent pas être identifiés ou ne s'y attendent pas.

Les caractéristiques biométriques représentent effectivement des renseignements personnels; votre visage, vos empreintes digitales ou les caractéristiques de votre iris, c'est vous. Par extension, toutes les données dérivées de votre visage ou d'une autre caractéristique biométrique employée pour confirmer votre identité représentent aussi des renseignements personnels. Vous jouissez du droit à la protection de ces données biométriques.

Certaines caractéristiques biométriques sont visibles partout et semi-publiques; par exemple, tout le monde peut voir votre visage, vous laissez des empreintes digitales sur tout ce que vous touchez et vous laissez partout où vous allez des matières contenant votre ADN. La biométrie recèle des commodités et avantages précieux; par exemple, elle permet de capturer des criminels ou de sécuriser l'accès à des lieux et à des ressources électroniques. Nous approchons rapidement l'ère où nos activités quotidiennes, nos déplacements et nos comportements seront automatiquement identifiés, retracés et profilés au moyen de la biométrie, à notre insu et sans notre consentement.

Heureusement, il existe des solutions pour protéger la vie privée, mais elles doivent être intégrées dès l'instauration du système de jumelage biométrique pour être efficaces. Lorsqu'il est déployé correctement, le chiffrement biométrique (CB) permet de répondre à bon nombre des principales préoccupations qui entourent la collecte et l'usage ou l'abus de caractéristiques biométriques, car aucune image biométrique ni modèle n'est conservé, ce qui améliore considérablement la sécurité et réduit le risque qu'une correspondance soit établie avec le contenu d'autres bases de données. Le CB peut être déployé sans réduire la fonctionnalité des systèmes.

PROJET DE LA SOCIÉTÉ DES LOTERIES ET DES JEUX DE L'ONTARIO

Le défi consistait à élaborer un système de reconnaissance faciale pour les casinos et les établissements de jeu qui permette d'identifier les 15 000 participants à un programme volontaire d'autoexclusion destiné aux joueurs problématiques, tout en protégeant la vie privée des centaines de milliers d'autres clients qui ne participent pas à ce programme.

L'objectif de ce projet était double : protéger la vie privée de toutes les personnes photographiées, tant celles qui figurent dans la base de données que celles qui visitent les établissements de la Société des loteries et des jeux de l'Ontario, et déceler avec un taux élevé de précision, grâce au système de reconnaissance faciale, les personnes inscrites au programme d'autoexclusion. Il était important aussi de protéger et de sécuriser les données existantes et nouvelles; ainsi, personne ne verrait son identité révélée si les renseignements tombaient entre de mauvaises mains.

Les fonctionnalités de protection de la vie privée du système ont été conçues par des ingénieurs en biométrie du département de génie électrique et informatique de l'Université de Toronto, sous la direction du professeur Kostas Plataniotis en collaboration avec Karl Martin, et mises au point de concert avec iView Systems, concepteur de systèmes de surveillance vidéo et de biométrie.

Cette technologie innovante, associée à des éléments photographiques modifiés, permet d'assurer un taux d'identification inégalé de 91 p. 100. Un projet pilote mené en Allemagne en 2007 avait atteint un taux de 30 à 60 p. 100; cette solution ontarienne est donc le système à chiffrement biométrique qui assure la meilleure protection de la vie privée dans le monde.

Votre appareil mobile, c'est vous

L'avènement des appareils de communication mobiles rappelle celui des ordinateurs personnels. Ces appareils posent de très lourds défis sur le plan de la sécurité de l'information, de la protection de la vie privée, de la convivialité et de la fonctionnalité. L'an dernier, des histoires d'horreur ont circulé dans les médias à la suite d'atteintes à la vie privée sur des appareils mobiles :

- Copie et enregistrement secrets des données de localisation;
- Réglages implicites lacunaires pour les services géodépendants;
- Applications trompeuses ou malveillantes;
- Découverte de programmes malveillants furtifs sur des appareils mobiles;
- Piratage de carnets d'adresses.

L'écosystème mobile dans son ensemble fait l'objet d'une attention sans précédent de la part du public et des organismes de réglementation, qui s'intéressent aux pratiques des intervenants en matière de gestion de l'information et de protection de la vie privée, et cela n'a rien d'étonnant, car les appareils mobiles révèlent des renseignements très personnels sur leurs propriétaires.

En partie en raison de la révélation de pratiques portant atteinte à la vie privée et d'un manque de transparence, des études sur les pratiques mobiles actuelles ont été menées et publiées l'an dernier. Des lignes directrices facultatives pour le secteur mobile ont été élaborées sous l'égide du Future of Privacy Forum, de la GSMA, du Center for Democracy and Technology, de la Digital Advertising Alliance ainsi que de la Commission fédérale du commerce et de la

Commission fédérale des communications des États-Unis, entre autres organismes.

En décembre 2010, j'ai abordé le sujet en publiant *The Roadmap for Privacy by Design in Mobile Communications: A Practical Tool for Developers, Service Providers, and Users*, un document qui résume les risques pour la vie privée dans l'écosystème mobile, les défis à relever et des solutions possibles. Fruit d'un atelier d'experts convoqué par la professeure Marilyn Prosch du laboratoire de l'Université de l'Arizona sur la *protection de la vie privée intégrée*, ce document divise les risques pour la vie privée en six catégories et propose plus d'une vingtaine de recommandations liées à la *PIVP* à l'intention des fabricants d'appareils, des réalisateurs de systèmes d'exploitation et de plateformes, des fournisseurs de réseaux, des concepteurs et distributeurs d'applications et des consommateurs, qui sont les intervenants clés de l'écosystème mobile.

Nous avons abordé également les risques systémiques dans notre document de juin 2011 intitulé *Wi-Fi Positioning Systems: Beware of Unintended Consequences*, qui aborde les problèmes que peut causer une infrastructure de communication sans fil qui, de façon implicite, peut révéler l'identité, l'emplacement et le comportement des appareils qui y sont reliés.

À l'été 2011, nous avons été les hôtes, avec l'American Civil Liberties Union et le Tor Project, du tout premier concours pour réalisateurs d'applications mobiles appelé *Developer Challenge for Mobile Apps*, qui visait à motiver ces réalisateurs à combler les lacunes des appareils mobiles sur le plan de la protection de la vie privée. Les résultats de ce concours ont été annoncés à Las Vegas aux conférences sur la sécurité DEFCON et Black Hat.

En septembre 2011, nous avons publié *Safeguarding Personal Health Information When Using Mobile Devices for Research Purposes*, qui donne aux dépositaires, aux chercheurs et aux commissions d'éthique de la recherche des renseignements leur permettant de comprendre et de remplir leurs obligations relativement à la protection des renseignements personnels sur la santé qui sont recueillis, utilisés et divulgués à des fins de recherche.

En novembre 2011, nous avons publié *Mobile Near Field Communications (NFC) "Tap 'n Go" — Keep it Secure & Private*, qui examine les technologies de communication en champ proche (NFC) et leur utilisation croissante dans les appareils mobiles, particulièrement les téléphones intelligents. Nous avons relevé les principaux risques pour la vie privée et la sécurité qui sont associés aux puces d'identification par radiofréquence et aux lecteurs de puces intégrés dans les téléphones mobiles, et nous avons proposé des solutions à l'intention des concepteurs d'appareils et des réalisateurs d'applications NFC qui s'appuient sur les principes fondamentaux de la *protection de la vie privée intégrée*.

La sensibilisation et l'information des utilisateurs, de même que la conception et la configuration appropriées des appareils, permettrait d'éliminer la plupart, voire tous, les risques pour la vie privée du côté des appareils mobiles, mais il reste d'autres risques et défis au niveau du système; pour y faire face, les intervenants de l'écosystème mobile devront faire preuve de coopération et viser la normalisations.

Accès à l'information intégré

J'ai élaboré le concept d'*accès à l'information intégré* (*AII*) parce que je voulais revoir la façon dont interagissent le gouvernement et les citoyens et encourager les institutions publiques à divulguer des renseignements de façon proactive et non réactive. En bref, je voulais que les gouvernements reconnaissent que l'information qu'ils détiennent est un bien public, et qu'il devrait être possible d'y accéder d'office, dans le cadre d'un processus automatique. Cependant, comme je l'ai déjà dit, l'*AII* va beaucoup plus loin que la simple divulgation systématique. Fondé sur sept principes fondamentaux, l'*AII* appelle le gouvernement à être plus réceptif et efficace, et à bâtir des rapports fondés sur la collaboration avec les citoyens, le secteur privé et d'autres institutions publiques. La nature tentaculaire du Web et des technologies connexes a fait croître considérablement la demande de renseignements détenus par le gouvernement au sein du public, donnant une nouvelle dimension à la participation civique et permettant un apport croissant des citoyens à l'élaboration des politiques et à la prestation des services.

J'ai également le plaisir de préciser qu'en 2011, mon bureau a rendu une ordonnance qui aborde certains des défis et principes associés à l'*AII*. L'ordonnance PO-3002, rendue le 14 octobre 2011, aborde la question des droits, qui est mentionnée dans le principe no 6 de l'*AII* : *Rendre l'information vraiment accessible.*

Dans cette affaire, l'appelant demandait l'accès à un rapport que la Commission de la location immobilière lui avait déjà fourni régulièrement et qui était produit par des moyens électroniques. Après avoir implanté un nouveau système électronique de gestion des cas, la Commission a voulu imposer des droits de 16 349 $ à l'appelant pour couvrir les coûts associés à la production du même rapport. En tant que commissaire, cette estimation des droits m'apparaissait tout à fait déraisonnable, et je l'ai rejetée en totalité. J'ai ordonné à la Commission de produire le rapport et de le remettre à l'appelant sans frais. J'ai précisé que je m'attendais à ce que la Commission fasse en sorte que l'instauration de nouveaux systèmes lui permette de continuer de produire le même rapport que par le passé.

Afin que l'information publique soit vraiment accessible, il faut éviter d'y faire obstacle en assujettissant notamment les demandes d'accès à l'information à des droits déraisonnables. On dit que l'information est le moteur de l'économie du XXIe siècle, mais elle permet aussi la participation concrète des citoyens à la vie publique. Non seulement il est essentiel pour les institutions gouvernementales de verser des données publiques dans des bases de données publiques, mais ces institutions doivent également s'assurer que ces données sont accessibles. Nous devons adopter cette nouvelle culture en rendant les données facilement accessibles au public et, comme ailleurs dans le monde, permettre aux secteurs public et privé de collaborer avec le gouvernement en utilisant ces données publiques, ce qui pourrait rapporter une foule d'avantages à la société et à l'économie dans son ensemble.

Les hôpitaux désormais assujettis à la *LAIPVP*

Mon bureau a passé une bonne partie de 2011 à communiquer avec les hôpitaux de toute la province pour les aider à se préparer à l'application de la *Loi sur l'accès à l'information et la protection de la vie privée* (*LAIPVP*), à laquelle ils sont assujettis depuis le 1er janvier 2012. Il s'agit d'une étape historique dans l'évolution de l'accès à l'information en Ontario, car les citoyens de l'Ontario jouissent désormais de l'accès à un vaste éventail de documents détenus par des institutions financées par les deniers publics.

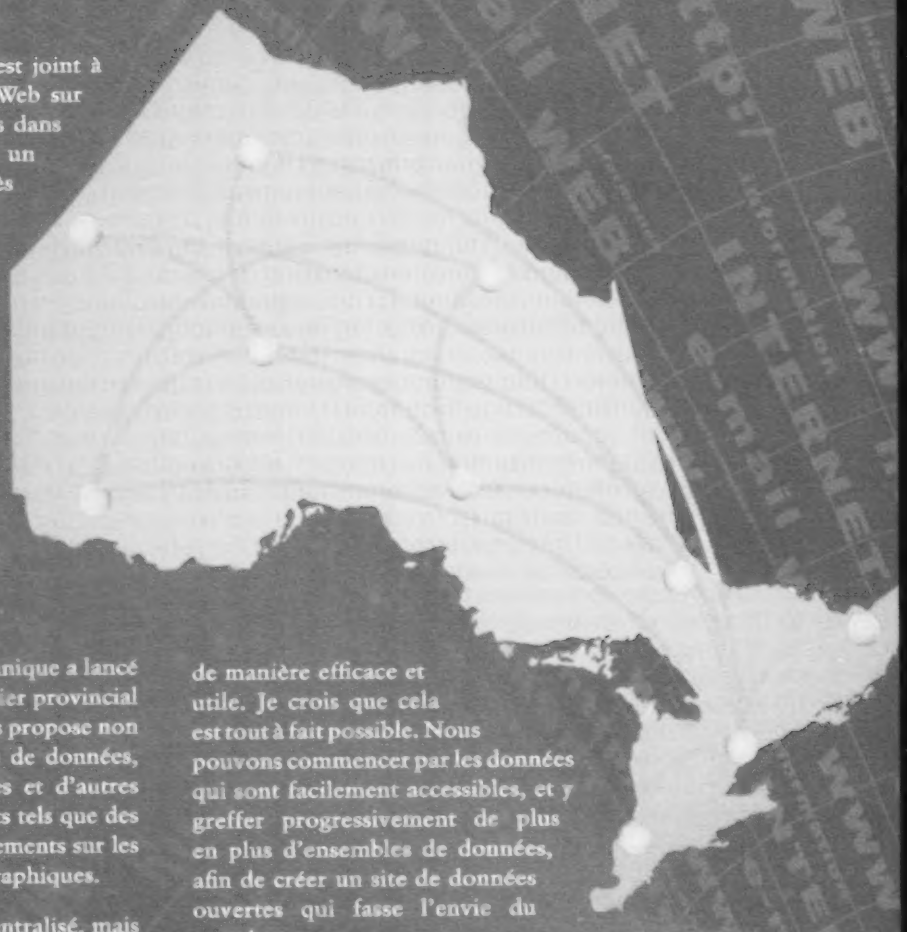
Pour aider les hôpitaux à se préparer à l'application de la *Loi*, mon bureau a publié deux documents au début de 2011. Le premier, *Application de la LPRPS et la LAIPVP aux renseignements personnels sur la santé : Directives à l'intention des hôpitaux*, les renseigne sur l'application de la *LPRPS* et de la *LAIPVP* aux renseignements personnels sur la santé dans le contexte de leurs activités. Le second, *Les hôpitaux et l'accès à l'information : Questions fréquentes*, répond aux questions les plus courantes sur l'application de la législation, notamment : Quand les dispositions sur l'accès à l'information s'appliqueront-elles aux hôpitaux? Pourquoi les hôpitaux ont-ils été ajoutés en vertu de la loi? Quels sont les changements qui sont apportés avec l'ajout des hôpitaux à la *LAIPVP*?

Mon personnel et moi avons également fait des exposés et rencontré des dirigeants d'hôpitaux pour nous assurer qu'ils étaient prêts à apporter les changements nécessaires. Parmi les organismes avec qui nous avons collaboré, mentionnons l'Association des hôpitaux de l'Ontario, le Centre de santé Trillium, le Réseau universitaire de santé, l'Hôpital Mount Sinai, l'Hôpital St. Michael et le Hospital for Sick Children. En outre, nous sommes allés au-delà de la région du grand Toronto et nous avons communiqué avec plus d'une dizaine d'hôpitaux de la province pendant la *Semaine du droit à l'information 2011* en tenant des tables d'information. Ce fut une tâche ardue pour mon personnel compte tenu du territoire à couvrir, mais nous sommes parvenus à faire comprendre aux hôpitaux et à leur personnel que l'application de la loi ne nuirait pas à la prestation des soins de santé, mais qu'elle permettrait d'ajouter de la légitimité à leurs activités en rendant nos institutions publiques plus transparentes et plus comptables à la population.

Données ouvertes

D'année en année, de plus en plus de territoires dans le monde se joignent au mouvement des données ouvertes, une initiative qui s'appuie essentiellement sur le concept selon lequel certains types de renseignements détenus par le gouvernement *qui ne sont pas des renseignements personnels* devraient être mis à la disposition de quiconque souhaite les utiliser et les republier. La nature tentaculaire du Web et des technologies connexes a fait croître considérablement la demande de renseignements détenus par le gouvernement au sein du public, donnant une nouvelle dimension à la participation civique et redéfinissant l'importance des lois sur l'accès à l'information.

Il existe tellement de données sous des formes si variées que les particuliers, groupes communautaires et chercheurs peuvent désormais utiliser des renseignements publics à une variété de fins; par exemple, relever des cas d'inefficacité dans les services gouvernementaux, et formuler des recommandations directement aux bureaux responsables de ces services. C'est avantageux sur le plan économique car les entreprises ont accès à une foule de renseignements sur lesquels se fonder pour améliorer leurs produits et services ou créer de tout nouveaux.



En 2011, le gouvernement du Canada s'est joint à plusieurs autres pays en lançant un site Web sur son Projet pilote sur les données ouvertes dans le cadre de son engagement d'assurer un gouvernement ouvert. Ce site donne accès à de vastes ensembles de données sur des sujets tels que l'immigration, la foresterie et le transport.

Plusieurs municipalités de l'Ontario disposent également de portails de données ouvertes. À ce titre, la ville de Toronto donne l'exemple avec un site Web de calibre mondial, DataTO.org un site simple et efficace où l'on peut trouver et télécharger des ensembles de données contenant une quantité incroyable de renseignements sur presque tous les sujets qui intéressent la ville.

À l'échelon provincial, la Colombie-Britannique a lancé le premier site de données ouvertes de palier provincial au Canada, DataBC. Ce portail de données propose non seulement un grand nombre d'ensembles de données, mais aussi des applications informatiques et d'autres programmes contenant des renseignements tels que des données environnementales, des renseignements sur les services judiciaires et des données démographiques.

L'Ontario reste sans portail de données centralisé, mais on a beaucoup parlé de la possibilité d'en créer un au cours de la dernière année. Je crois que l'Ontario doit établir son propre portail de données ouvertes afin de montrer qu'il demeure un chef de file mondial de l'accès à l'information.

Le gouvernement 2.0 est axé en bonne partie sur la participation des citoyens. Il est donc temps que l'Ontario entame le XXI[e] siècle en fournissant des données ouvertes et en conférant à tous ses citoyens le droit à un gouvernement ouvert. Je crois que le gouvernement de l'Ontario pourrait mettre en ligne un site centralisé de données ouvertes d'ici la fin de 2012, et je l'encourage vivement à le faire. L'usage d'outils tels que des wikis, des blogues, des sites de cartographie en ligne et d'autres applications pousse les gouvernements à fournir des données à leurs citoyens de manière efficace et utile. Je crois que cela est tout à fait possible. Nous pouvons commencer par les données qui sont facilement accessibles, et y greffer progressivement de plus en plus d'ensembles de données, afin de créer un site de données ouvertes qui fasse l'envie du monde.

La *LPRPS* en 2011

Voici des faits saillants sur l'application en 2011 de la *Loi sur la protection des renseignements personnels sur la santé* (*LPRPS*), que mon bureau supervise depuis son adoption en 2004.

Ordonnance en matière de santé n° 11 (HO-011) – Action Cancer Ontario

Après la perte de rapports de dépistage contenant des renseignements personnels sur la santé sur plus de 7 000 Ontariennes et Ontariens, j'ai rendu, le 13 octobre 2011, l'ordonnance en matière de santé n° 11 (HO-011) ordonnant à Action Cancer Ontario de cesser d'envoyer par messager des rapports de dépistage sur papier contenant des renseignements personnels sur la santé à des médecins de soins primaires.

J'ai rendu l'ordonnance HO-011 en m'appuyant sur un certain nombre de facteurs, notamment la taille, les ressources et le raffinement des procédés d'Action Cancer Ontario (ACO), les personnes ou organismes à qui les dossiers de renseignements personnels sur la santé étaient transférés (ils étaient transférés à des médecins de soins primaires plutôt qu'à des personnes qui ne disposaient pas nécessairement de la technologie nécessaire pour accéder aux renseignements sous forme électronique), l'accessibilité de méthodes de rechange pour assurer le transfert sécurisé des dossiers de renseignements personnels sur la santé sous forme électronique, le nombre de personnes dont les renseignements personnels sur la santé étaient contenus dans les dossiers (un seul rapport de dépistage contenait des renseignements sur plusieurs personnes), et le fait que le transfert se faisait dans le cadre d'un programme à long terme à l'échelle provinciale faisant intervenir de grandes quantités de renseignements personnels sur la santé.

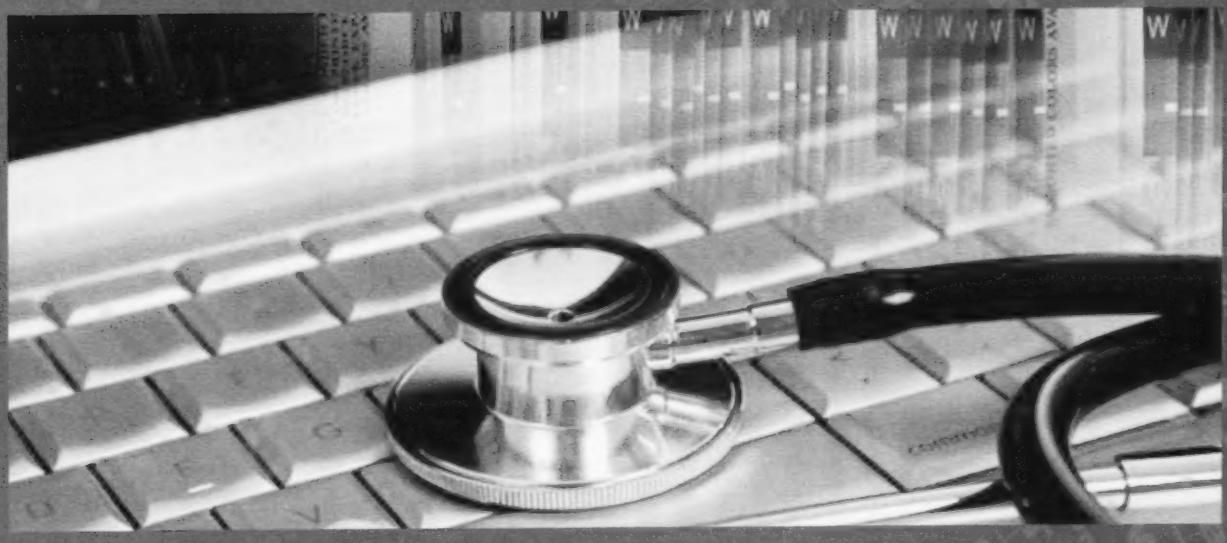
J'ai le plaisir de confirmer qu'ACO a immédiatement cessé de transférer des rapports de dépistage sur papier par messager et a collaboré pleinement à l'examen. Cet organisme envisage de transmettre ces rapports par un moyen électronique sécurisé aux médecins de soins primaires. ACO a aussi revu et modifié ses politiques et procédures de gestion des atteintes à la vie privée et fourni de la formation supplémentaire sur la protection de la vie privée pour s'assurer que ses employés et les personnes avec qui il a une relation contractuelle ou autre sont bien mis au courant de leur responsabilité de signaler aussitôt à des responsables toute atteinte à la vie privée réelle ou éventuelle et tout risque pour la vie privée.

L'ordonnance HO-011 souligne la nécessité, pour les intervenants du secteur de la santé, d'évaluer soigneusement les possibilités qui s'offrent à eux, y compris les solutions technologiques, pour assurer la sécurité et la confidentialité des dossiers de renseignements personnels sur la santé qu'ils transfèrent.

Examen et approbation des entités et personnes prescrites

Mon bureau a achevé l'examen triennal prévu par la loi des pratiques relatives aux renseignements de quatre entités prescrites et de trois personnes prescrites qui dressent ou tiennent des registres de renseignements personnels sur la santé, en suivant le nouveau processus simplifié que mon bureau a établi en 2010 et qui est décrit dans le *Manual for the Review and Approval of Prescribed Persons and Prescribed Entities*. Ces entités prescrites sont Action Cancer Ontario, l'Institut canadien d'information sur la santé, l'Institut de recherche en services de santé et le Pediatric Oncology Group of Ontario. Les personnes prescrites, quant à elles, sont le Réseau ontarien de soins cardiaques en ce qui concerne le registre de services cardiaques, INSCYTE (Information System for Cytology) Corporation en ce qui concerne le système CytoBase et Action Cancer Ontario en ce qui concerne le Registre ontarien de dépistage du cancer. Ce nouveau processus s'applique uniquement aux personnes et entités prescrites qui ont déjà fait examiner et approuver leurs pratiques relatives aux renseignements par mon bureau.

En 2011, mon bureau a également examiné et approuvé les pratiques relatives aux renseignements de deux nouvelles personnes prescrites : le Centre hospitalier pour enfants de l'est de l'Ontario en ce qui concerne le Registre et réseau des Bons résultats dès la naissance, et l'Institut ontarien de recherche sur le cancer en ce qui concerne la Banque de tumeurs de l'Ontario. Ces nouvelles personnes prescrites ont été tenues de faire examiner et approuver toutes les pratiques et procédures applicables qu'elles ont mises en œuvre en vue de protéger la vie privée des particuliers dont elles reçoivent des renseignements personnels sur la santé et d'assurer la confidentialité de ces renseignements. Mon bureau a également effectué des visites sur place pour s'assurer que les précautions appropriées avaient été prises pour protéger les renseignements personnels sur la santé que les nouvelles personnes prescrites recueillent, utilisent et divulguent.



Bien qu'en 2006, Hamilton Health Science Corporation soit devenue une personne prescrite qui dresse ou tient le registre du Système d'information sur les soins aux malades en phase critique, elle n'a pas encore fait examiner ou approuver ses pratiques relatives aux renseignements par mon bureau. Par conséquent, les dépositaires de renseignements sur la santé ne sont pas encore autorisés à lui divulguer des renseignements personnels sur la santé aux fins de l'alinéa 39 (1) c) de la *LPRPS* sans le consentement du particulier.

Règlement concernant Cybersanté Ontario

Mon bureau a été consulté concernant des modifications proposées au Règlement 329/04 pris en application de la *LPRPS* afin de permettre à Cybersanté Ontario d'accéder à des renseignements personnels sur la santé en tant que fournisseur de services qui crée ou tient des dossiers de santé électroniques (DSE). À la suite de ces consultations, le Règlement 329/04 a été modifié afin d'autoriser les dépositaires de renseignements sur la santé à fournir des renseignements personnels sur la santé à Cybersanté Ontario pour lui permettre de créer ou de tenir un ou plusieurs DSE dans la mesure où cet organisme répond aux exigences énumérées à l'article 6.2 de ce règlement, notamment effectuer une évaluation des menaces, de la vulnérabilité et des risques qui existent en matière de protection et d'intégrité des renseignements personnels sur la santé contenus dans le dossier de santé électronique et une évaluation de l'impact possible sur la vie privée.

Renseignements à l'intention des chercheurs en soins de santé

En 2011, mon bureau a publié deux documents dans le but d'orienter les chercheurs en santé sur les mesures qu'ils peuvent prendre afin de rehausser la protection de la vie privée et de se conformer à la *LPRPS*.

Le premier de ces documents, *Dispelling the Myths Surrounding De-identification: Anonymization Remains a Strong Tool for Protecting Privacy*, publié en juin, a été rédigé en collaboration avec le Dr Khaled El Emam, titulaire de la chaire de recherche du Canada sur les données électroniques en matière de santé à l'Université d'Ottawa, et de l'Institut de recherche du Centre hospitalier pour enfants de l'est de l'Ontario. Ce document chasse certains mythes sur l'anonymisation des renseignements personnels sur la santé, qu'il préconise comme l'une des mesures les plus importantes à prendre pour protéger la vie privée dans le contexte de l'utilisation de tels renseignements à des fins autres que la prestation de soins de santé, comme la recherche.

Le second document, *Safeguarding Personal Health Information When Using Mobile Devices for Research Purposes*, a été publié en septembre; il aide les dépositaires de renseignements sur la santé, les chercheurs et les commissions d'éthique de la recherche à comprendre et à respecter leurs obligations en matière de protection des renseignements personnels sur la santé qui sont recueillis, utilisés et divulgués à des fins de recherche.

Demandes d'accès à l'information, selon l'ordre de gouvernement et le genre de document

	Renseignements personnels	Documents généraux	Total
Municipal	13 535	14 466	28 001
Provincial	5 221	11 937	17 158
Total	18 756	26 403	45 159

Un nombre record de demandes d'accès à l'information a été présenté en Ontario en 2011 : 45 159, dépassant de 16 p. 100 l'ancien record de 38 903 établi en 2010.

Les organismes provinciaux ont reçu 17 158 demandes en 2011, soit une hausse de 13,1 p. 100 par rapport aux 15 161 demandes reçues en 2010. De ce nombre, 5 221 (30,4 p. 100) étaient des demandes d'accès à des renseignements personnels concernant l'auteur de la demande, et 11 937 (69,6 p. 100) des demandes d'accès à des documents généraux.

Le ministère de l'Environnement a continué de recevoir le plus grand nombre de demandes en vertu de la *Loi* provinciale – 6 111 en 2011, en hausse de 580 par rapport à 2010. Comme c'est le cas depuis quelques années, les autres ministères ayant reçu le plus de demandes ont été le ministère de la Sécurité communautaire et des Services correctionnels (4 873), le ministère des Services sociaux et communautaires (1 338, soit 58,6 p. 100 de plus que les 785 demandes reçues en 2010) et le ministère du Travail (925). Ensemble, ces quatre ministères ont continué de recevoir la grande majorité des demandes, soit 77 p. 100 de toutes les demandes provinciales en 2011.

Les organismes des administrations municipales ont reçu 28 801 demandes d'accès à l'information en 2011, une hausse de 21,3 p. 100 par rapport aux 23 742 demandes reçues en 2010. Les demandes adressées aux municipalités ont continué d'augmenter, passant de 19 887 en 2008 à 28 801 en 2011. Parmi les demandes d'accès à l'information présentées aux institutions municipales en 2011, 13 535 (47,0 p. 100) concernaient des renseignements personnels et 14 446 (53,0 p. 100) des documents généraux.

Parmi les dix institutions municipales ayant reçu le plus de demandes d'accès à l'information, six étaient des commissions de services policiers, qui ont continué de recevoir de loin le plus de demandes en vertu de la *Loi* municipale, soit 16 834 (58,4 p. 100). Les municipalités sont arrivées au deuxième rang avec 10 615 demandes, suivies des conseils scolaires avec 240 demandes et des conseils de santé avec 58 demandes.

Les droits moyens que les institutions provinciales ont exigés pour l'accès à des documents généraux en 2011 ont augmenté légèrement pour s'établir à 41,39 $, ce qui reste bien inférieur à la moyenne record de plus de 51 $ enregistrée en 2006.

On trouvera les statistiques complètes sur les demandes d'accès à l'information présentées en 2011 à www.ipc.on.ca.

Coût moyen des demandes provinciales

	2007	2008	2009	2010	2011
Renseignements personnels	10,54 $	11,26 $	9,47 $	12,88 $	11,35 $
Documents généraux	50,54 $	42,74 $	39,66 $	39,97 $	41,39 $

Coût moyen des demandes municipales

	2007	2008	2009	2010	2011
Renseignements personnels	9,67 $	8,82 $	8,11 $	8,01 $	8,83 $
Documents généraux	23,49 $	23,54 $	26,55 $	25,68 $	24,22 $

Respect du délai de réponse

Dix premières institutions provinciales, selon le nombre de demandes réglées

	Demandes reçues	Demandes réglées	Dans un délai de 30 jours	%	Délai prolongé	Plus de 90 jours	%
Ministère de l'Environnement	6 111	5 935	4 876	82,2 %	5 073	321	5,4 %
Ministère de la Sécurité communautaire et des Services correctionnels	4 873	4 692	3 971	84,6 %	4 464	138	2,9 %
Ministère des Services sociaux et communautaires	1 338	1 264	999	79,0 %	1 010	26	2,1 %
Ministère du Travail	925	885	813	91,9 %	813	14	1,6 %
Archives publiques de l'Ontario	474	446	382	85,7 %	439	3	0,7 %
Ministère du Procureur général	442	411	384	93,4 %	393	6	1,5 %
LCBO	376	393	382	97,2 %	382	0	0,0 %
Ministère des Transports	377	353	328	92,9 %	334	3	0,8 %
Commission de la location immobilière	317	344	336	97,7 %	336	0	0,0 %
Société des loteries et des jeux de l'Ontario	229	222	210	94,6 %	222	1	0,5 %

*Comprenant les cas où un avis de prorogation du délai [paragraphe 27 (1)] ou un avis à la personne concernée [paragraphe 28 (1)] a été donné. Ces avis sont utilisés lorsque, par exemple, il est nécessaire de fouiller un grand nombre de documents ou de consulter une ou plusieurs personnes de l'extérieur de l'organisme.

Mon bureau publie les taux de respect afin de souligner l'importance pour les organismes gouvernementaux de respecter le délai de réponse aux demandes d'accès à l'information prévu dans les *Lois* (bien que le respect de ce délai ne puisse, à lui seul, rendre compte pleinement de la qualité des réponses à ces demandes). Le taux de respect des institutions provinciales du délai de réponse de 30 jours a continué d'augmenter, passant de 42 p. 100 à plus de 80 p. 100 depuis 1999, année où le CIPVP a commencé à publier le taux de respect de diverses institutions.

Institutions régies par la *Loi* provinciale

Le taux de respect du délai de réponse de 30 jours des ministères, organismes et autres institutions de palier provincial a fléchi légèrement en 2011, s'élevant à 83,6 p. 100 par rapport au sommet de 85 p. 100 atteint en 2008. La plupart des demandes, soit 11 170 (65,1 p. 100), émanaient d'entreprises, et 4 223 (24,6 p. 100) de particuliers.

Le taux de respect du délai de réponse prolongé des institutions provinciales est demeuré stable en 2011, s'élevant à 90,0 p. 100, ce qui est inférieur au record de 97,2 p. 100 enregistré en 2009. Le délai prolongé permet aux institutions de répondre à une demande dans un délai plus long que celui de 30 jours en raison de circonstances atténuantes précises. Ce taux est calculé depuis 2002 seulement.

Institutions régies par la *Loi* municipale

Les institutions municipales ont affiché un taux de respect du délai de réponse de 30 jours aux demandes d'accès à l'information inférieur à celui des institutions provinciales, soit 80,1 p. 100. Si l'on tient compte des demandes dont le délai de réponse a été prolongé, le taux de réponse atteint 83,5 p. 100, une baisse de 4,9 points de pourcentage par rapport à 2010. La plupart des demandes, soit 18 398 (67,7 p. 100) émanaient de particuliers, suivies des entreprises avec 7 304 demandes (26,8 p. 100).

Depuis 2009, les Services de police de Toronto sont l'institution municipale qui répond au plus grand nombre de demandes d'accès à l'information; en 2011, ils ont répondu à 4 862 demandes, et leur taux de respect du délai de réponse de 30 jours a été de 76,3 p. 100 (79,4 p. 100 en tenant compte des demandes dont le délai de réponse a été prolongé). La ville de Toronto, qui occupait auparavant le premier rang quant au nombre de demandes d'accès à l'information reçues, a répondu à 2 386 demandes avec un taux de respect du délai de réponse de 30 jours de 82,5 p. 100 (88,2 p. 100 en tenant compte des demandes dont le délai de réponse a été prolongé). La Commission des services policiers de la région de Peel est demeurée au troisième rang, en répondant à 1 501 demandes. Cependant, pour la première fois depuis 2008, elle n'a pas obtenu un taux parfait de respect du délai de réponse de 30 jours et du délai prolongé; dans les deux cas, elle a affiché un taux de 83,5 p. 100 en 2011.

Les taux de réponse des ministères, des municipalités, des corps de police, des conseils scolaires, etc. pour 2011 se trouvent à www.ipc.on.ca.

Sommaire des appels – 2011 par rapport à 2010

2011	Documents généraux			Renseignements personnels			Total		
	Provincial	Municipal	Total	Provincial	Municipal	Total	Provincial	Municipal	Total
Dossiers ouverts	468	333	801	154	259	413	623	591	1 214
Dossiers fermés	337	296	633	145	245	390	483	540	1 023

2010	Documents généraux			Renseignements personnels			Total		
	Provincial	Municipal	Total	Provincial	Municipal	Total	Provincial	Municipal	Total
Dossiers ouverts	328	306	634	121	222	343	449	528	977
Dossiers fermés	257	302	559	139	218	357	396	520	916

Les personnes qui ont présenté une demande écrite d'accès à l'information en vertu de la *Loi sur l'accès à l'information et la protection de la vie privée* ou de la *Loi sur l'accès à l'information municipale et la protection de la vie privée* mais sont insatisfaites de la réponse qu'elles ont reçue peuvent en appeler au CIPVP. Les appels peuvent porter sur le refus d'accorder l'accès, le montant des droits demandés, le non-respect du délai de réponse prescrit de 30 jours, le refus de rectifier les renseignements personnels concernant l'auteur de la demande ou d'autres aspects touchant la procédure de traitement des demandes.

Appels en 2011

En 2011, 1 214 appels ont été interjetés devant le CIPVP, un nombre record. Au total, 1 023 appels ont été réglés en 2011, 107 de plus qu'en 2010.

Les documents qui ne contiennent pas de renseignements personnels sur l'auteur de la demande sont appelés des documents généraux. En 2011, 801 appels concernant l'accès à des documents généraux ont été déposés au CIPVP : 468 en vertu de la *Loi* provinciale et 333 en vertu de la *Loi* municipale.

Le CIPVP a reçu 413 appels concernant des renseignements personnels en 2011, dont 154 en vertu de la *Loi* provinciale et 259 en vertu de la *Loi* municipale.

En 2011, le nombre d'appels déposés en vertu de la *Loi* municipale a augmenté de 63 pour s'établir à 591, et le nombre de ceux déposés en vertu de la *Loi* provinciale a augmenté de 174 pour atteindre 623 par rapport à l'année précédente.

Sur les 623 appels déposés à mon bureau en vertu de la *Loi* provinciale, 151 (33,6 p. 100) impliquaient le ministère de la Santé et des Soins de longue durée et 123 (27,4 p. 100) le ministère de la Sécurité communautaire et des Services correctionnels. Vingt-cinq autres appels concernaient des décisions du ministère des Services gouvernementaux, suivi du ministère du Procureur général (24) et des ministères des Richesses naturelles (19) et de l'Environnement (12). C'est l'Université d'Ottawa qui a fait l'objet du plus grand nombre d'appels parmi tous les organismes provinciaux avec 17, suivie de la Société des loteries et des jeux de l'Ontario avec 10.

Sur les 591 appels déposés au CIPVP en vertu de la *Loi* municipale, 275 (46,5 p. 100) impliquaient des services de police et 226 (38,2 p. 100) des municipalités. Les Services de police de Toronto, qui ont reçu à nouveau plus de demandes en vertu de la *Loi* municipale que tout autre organisme, ont également fait l'objet du plus grand nombre d'appels en vertu de la *Loi* (82), suivis de la ville de Toronto (48), des Services de police de la région de Halton (34), des Services de police de Hamilton (22), du Service de police d'Ottawa (19), des Services de police de la région de York (19) et de la ville d'Ottawa (12).

Le Toronto District School Board a fait l'objet du plus grand nombre d'appels à l'endroit d'un conseil scolaire (neuf), suivi du Hamilton-Wentworth District School Board (huit).

Pour des précisions sur les appels déposés et réglés en 2011, consulter le supplément statistique qui accompagne le présent rapport annuel à www.ipc.on.ca.

Plaintes concernant la protection de la vie privée

Sommaire des plaintes

	Plaintes déposées en 2010				Plaintes déposées en 2011			
	Provincial	Municipal	Hors-compétence	Total	Provincial	Municipal	Hors-compétemce	Total
Dossiers ouverts	127	125	0	252	131	135	0	266
Dossiers fermés	130	137	0	267	129	148	0	277

La *Loi sur l'accès à l'information et la protection de la vie privée* et la *Loi sur l'accès à l'information municipale et la protection de la vie privée* régissent la collecte, la conservation, l'utilisation, la divulgation, la sécurité et l'élimination des renseignements personnels que détiennent les institutions gouvernementales.

Les personnes qui estiment qu'un organisme provincial ou municipal a porté atteinte à leur vie privée peuvent déposer une plainte à mon bureau en vertu des *Lois*. Dans la plupart des cas, mon bureau tentera de régler le différend par voie de médiation. Il peut également recommander officiellement à un organisme gouvernemental de modifier ses pratiques.

Plaintes concernant la protection de la vie privée

Le CIPVP a fermé le nombre record de 277 dossiers de plainte concernant la protection de la vie privée en 2011, dépassant de 10 le record précédent de 267 dossiers fermés en 2010.

Sur les 277 dossiers de plainte fermés en vertu des *Lois* s'appliquant au secteur public en 2011, 148 l'ont été en vertu de la *Loi* municipale et 129 en vertu de la *Loi* provinciale. Le CIPVP a également fermé 214 dossiers de plainte concernant la *collecte*, l'*utilisation* ou la *divulgation* de renseignements personnels sur la santé en vertu de la *Loi sur la protection des renseignements personnels sur la santé* (*LPRPS*), portant à 491 le nombre total de dossiers de plainte concernant la protection de la vie privée qui ont été fermés en 2011.

En 2011, 266 dossiers de plainte concernant la protection de la vie privée ont été ouverts en vertu des *Lois* s'appliquant au secteur public, le total le plus élevé depuis que la première de ces *Lois*, la *Loi sur l'accès à l'information et la protection de la vie privée*, est entrée en vigueur en 1988.

Sur les 266 dossiers de plainte ouverts en 2011, 131 l'ont été en vertu de la *Loi* provinciale et 135 en vertu de la *Loi* municipale. Si l'on tient compte des 223 plaintes concernant la *collecte*, l'*utilisation* ou la *divulgation* de renseignements personnels sur la santé déposées en vertu de la *LPRPS*, le nombre total de plaintes concernant la protection de la vie privée déposées au CIPVP en 2011 s'élève à 489, soit 11,1 p. 100 de plus que l'année précédente.

Comme c'est le cas depuis des années, le motif de plainte le plus souvent invoqué en vertu des deux *Lois* s'appliquant au secteur public était la divulgation de renseignements personnels. La divulgation a été invoquée dans 139 des plaintes réglées (63,2 p. 100). En outre, 27 plaintes (12,3 p. 100) avaient trait à la sécurité, et la collecte de renseignements personnels était en cause dans 17 cas (7,7 p. 100). Les autres plaintes portaient sur des questions telles que la conservation, l'utilisation, les avis de collecte et l'élimination.

Mon bureau continue de privilégier le règlement informel des litiges. J'ai le plaisir d'annoncer qu'en 2011, 97,1 p. 100 des plaintes concernant la protection de la vie privée ont été réglées sans qu'un rapport officiel ne soit publié ni qu'une ordonnance ne soit rendue.

Parmi les plaintes réglées, 166 (près de 60 p. 100) avaient été déposées par des particuliers, et 11 (4 p. 100) par la commissaire. Cent autres (environ 36,1 p. 100) ont été déposées par les institutions elles-mêmes.

Pour des précisions sur les plaintes concernant la protection de la vie privée qui ont été déposées en 2011, voir le supplément statistique qui accompagne le présent rapport annuel à www.ipc.on.ca.

La *Loi sur la protection des renseignements personnels sur la santé (LPRPS)*

Sommaire – 2011 par rapport à 2010

	2010					2011				
	Collecte, utilisation ou divulgation					Collecte, utilisation ou divulgation				
	Accès ou rectification	Particuliers	Organismes	CIPVP	Total	Accès ou rectification	Particuliers	Organismes	CIPVP	Total
Dossiers ouverts	100	62	95	31	288	123	64	135	24	346
Dossiers fermé́d	112	59	98	22	291	109	64	123	27	323

Le nombre de plaintes déposées à mon bureau en vertu de la *Loi sur la protection des renseignements personnels sur la santé* (*LPRPS*) est passé à 346 en 2011, en hausse de 20 p. 100 par rapport aux 288 plaintes déposées en 2010 et le total le plus élevé au cours des sept années complètes d'application de la *LPRPS*.

Des hôpitaux publics étaient visés par 160 des 346 dossiers ouverts, soit environ 46,2 p. 100. De ces dossiers, 77 (57 p. 100) étaient des atteintes à la vie privée signalées par les hôpitaux eux-mêmes à la suite d'activités de collecte, d'utilisation ou de divulgation de renseignements personnels sur la santé. J'encourage activement les dépositaires de renseignements sur la santé à déclarer les incidents de ce genre, et mon bureau est déterminé à collaborer avec eux pour agir rapidement afin de prendre les mesures qui s'imposent.

Il y a eu 38 plaintes impliquant des médecins, en baisse par rapport aux 52 plaintes déposées en 2010, dont 17 avaient trait à l'accès aux renseignements personnels sur la santé ou à leur rectification. Le nombre de plaintes impliquant des cliniques est passé de 30 en 2010 à 35.

Dossiers fermés

Mon bureau a fermé 323 dossiers de plainte en 2011, soit 10 p. 100 de plus qu'en 2010 et 25 p. 100 de plus qu'en 2009. Fait notable en 2011, le nombre d'incidents signalés par les organismes concernés a augmenté, passant de 98 à 123, soit une hausse de 20 p. 100. Les 200 autres dossiers fermés en 2011 avaient trait à la collecte, à l'utilisation ou à la divulgation de renseignements personnels sur la santé. De ces dossiers, 64 ont été signalés par des particuliers, 123 par les organismes concernés et 27 par mon bureau.

Dans la mesure du possible, mon bureau privilégie le règlement des plaintes de façon informelle ou par médiation. Sur les 109 dossiers fermés concernant l'accès à des renseignements personnels sur la santé ou la rectification de ces renseignements, 69 (63 p. 100) ont été fermés de façon informelle au stade de la prise en charge, 36 (environ 33 p. 100) l'ont été au stade de la médiation et quatre (un peu plus de 3 p. 100) au stade de l'arbitrage.

Des 123 atteintes à la vie privée déclarées par les dépositaires de renseignements sur la santé eux-mêmes, 114 (plus de 92 p. 100) ont été réglées au stade de la prise en charge, huit au stade de la médiation et une au stade de l'arbitrage.

Des 64 plaintes déposées par des particuliers concernant la collecte, l'utilisation ou la divulgation de renseignements personnels sur la santé, 57 (environ 89 p. 100) ont été réglées au stade de la prise en charge, et six au stade de la médiation. Enfin, des 27 plaintes déposées par le CIPVP concernant la collecte, l'utilisation ou la divulgation de renseignements personnels sur la santé, 24 (plus de 88 p. 100) ont été réglées au stade de la prise en charge.

Demandes d'accès à des renseignements personnels sur la santé

Seuls les dépositaires de renseignements sur la santé qui sont assujettis également à la *LAIPVP* ou à la *LAIMPVP* sont tenus de signaler au CIPVP le nombre de demandes qu'ils ont reçues de la part de particuliers voulant obtenir des renseignements personnels sur la santé les concernant.

Les dépositaires ont dit avoir répondu à 7 822 de ces demandes en 2011. Le ministère de la Santé et des Soins de longue durée a répondu à 4 885 de ces demandes, soit plus de 62 p. 100. Il s'agissait là d'une baisse de 159 demandes par rapport aux 5 044 demandes reçues en 2010, soit un peu plus de 3 p. 100. Le ministère a pu répondre à 4 827 demandes, ou 98,9 p. 100, dans le délai de 30 jours prévu par la loi.

Types de dossiers concernant la LPRPS ouverts en 2011

			Collecte, utilisation ou divulgation							
	Accès ou rectification	%	Particuliers	%	Organismes	%	CIPVP	%	Total	%
Hôpitaux publics	52	42,3	26	40,6	77	57,0	5	20,8	160	46,2
Médecins	17	13,8	7	10,9	4	3,0	10	41,7	38	11,0
Cliniques	12	9,8	6	9,4	14	10,4	3	12,5	35	10,1
Centres, programmes ou services de santé communautaire ou de santé mentale	6	4,9	5	7,8	19	14,1	3	12,5	33	9,5
Autres professionnels de la santé	7	5,7	2	3,1	6	4,4	0	0,0	15	4,3
Centres d'accès aux soins communautaires	3	2,4	2	3,1	2	1,5	0	0,0	7	2,0
Ministère de la Santé	5	4,1	2	3,1	0	0,0	0	0,0	7	2,0
Établissements de soins de longue durée	4	3,3	0	0,0	1	0,7	1	4,2	6	1,7
Maisons de soins infirmiers	4	3,3	2	3,1	0	0,0	0	0,0	6	1,7
Mandataires	4	3,3	0	0,0	0	0,0	0	0,0	4	1,2
Services ambulanciers	0	0,0	1	1,6	3	2,2	0	0,0	4	1,2
Conseils de santé	0	0,0	1	1,6	2	1,5	0	0,0	3	0,9
Laboratoires	0	0,0	0	0,0	2	1,5	1	4,2	3	0,9
Autres	0	0,0	2	3,1	1	0,7	0	0,0	3	0,9
Autres personnes prescrites	2	1,6	1	1,6	0	0,0	0	0,0	3	0,9
Pharmacies	1	0,8	2	3,1	0	0,0	0	0,0	3	0,9
Dentistes	0	0,0	2	3,1	0	0,0	0	0,0	2	0,6
Ministre de la Santé	1	0,8	0	0,0	0	0,0	1	4,2	2	0,6
Psychologues	1	0,8	0	0,0	1	0,7	0	0,0	2	0,6
Maisons de soins - protection des locataires	1	0,8	0	0,0	0	0,0	0	0,0	1	0,3
Foyers de bienfaisance pour personnes âgées	0	0,0	0	0,0	1	0,7	0	0,0	1	0,3
Foyers ou foyers communs (personnes âgées ou maisons de repos)	1	0,8	0	0,0	0	0,0	0	0,0	1	0,3
Établissements de santé autonomes	0	0,0	1	1,6	0	0,0	0	0,0	1	0,3
Établissements aux termes de la *Loi sur les hôpitaux psychiatriques*	0	0,0	1	1,6	0	0,0	0	0,0	1	0,3
Infirmières	0	0,0	1	1,6	0	0,0	0	0,0	1	0,3
Physiothérapeutes	0	0,0	0	0,0	1	0,7	0	0,0	1	0,3
Entités prescrites	0	0,0	0	0,0	1	0,7	0	0,0	1	0,3
Techniciens en radiologie	1	0,8	0	0,0	0	0,0	0	0,0	1	0,3
Travailleurs sociaux	1	0,8	0	0,0	0	0,0	0	0,0	1	0,3
Total	**123**	**100,0**	**64**	**100,0**	**135**	**100,0**	**24**	**100,0**	**346**	**100,0**

Révisions judiciaires

Plusieurs décisions judiciaires rendues en 2011 ont souligné l'importance des *Lois*, qui permettent d'assurer la transparence et la responsabilité des pouvoirs publics dans une variété de contextes, notamment les dépenses et les décisions des municipalités, l'efficacité et les activités du gouvernement provincial ainsi que l'accès à des renseignements de tiers qui ne sont pas des renseignements personnels. Une décision a également réitéré l'importance de fournir des avis aux parties éventuellement concernées et de les traiter équitablement dans le cadre des processus prévus dans les *Lois*.

Ordonnance MO-2521 – *Vaughan (City) v. Ontario (Information and Privacy Commissioner)*[1]

La Cour divisionnaire de l'Ontario a confirmé la décision de mon bureau ordonnant à la ville de Vaughan de divulguer des copies des factures complètes de l'autoroute 407 ETR qu'elle a payées au cours d'une période de quatre ans pour les déplacements professionnels et personnels d'un employé. Auparavant, la ville avait divulgué des versions de ces factures montrant les montants payés, les dates où l'autoroute avait été empruntée et les distances parcourues, mais pas les points d'entrée et de sortie et les heures de la journée, soutenant qu'il s'agissait là de renseignements personnels concernant l'employé.

Mon bureau a jugé que les factures complètes divulgueraient « les avantages sociaux [...] d'un [...] employé » d'une institution au sens de 1'alinéa 14 (4) a) de la *LAIMPVP* et, par conséquent, que leur divulgation serait présumée ne pas représenter une atteinte injustifiée à la vie privée. Nous avons expliqué que les points d'entrée et de sortie permettent de déterminer le montant des droits de péage qui sont attribuables aux déplacements personnels et professionnels et, par conséquent, le montant des « avantages sociaux ». Nous avons également rejeté l'argument de la ville selon lequel il serait raisonnable de s'attendre à ce que la divulgation des allées et venues de l'employé compromette sa santé ou sa sécurité au sens de 1'article 13 de la *LAIMPVP*.

En examen judiciaire, la cour a souscrit fermement à la norme de contrôle judiciaire fondée sur le caractère raisonnable qui s'applique aux décisions du CIPVP portant sur la vie privée. Elle a rejeté l'argument de la ville selon lequel l'alinéa 14 (4) a) ne s'applique qu'à des descriptions générales des avantages sociaux énumérés dans un contrat de travail. La cour s'est penchée sur les objets de la loi fondés sur l'obligation redditionnelle et sur une décision antérieure de la Cour d'appel reconnaissant que la *LAIMPVP* ne vise pas à assurer une protection absolue de la vie privée. La cour a également cité d'autres décisions du CIPVP soulignant que les employés des municipalités sont comptables envers les contribuables de l'utilisation des fonds publics à des fins personnelles. Elle a confirmé la décision en la qualifiant de « raisonnable » tout en reconnaissant qu'elle parvenait à un équilibre satisfaisant en 1'occurrence.

Statistiques sur les révisions judiciaires de 2011

Nouvelles requêtes en révision judiciaire reçues en 2011 :	**2**
Requérant :	
Institutions[2]	1
Auteurs de demande	0
Parties conçernées	0
Intervention du CIPVP dans la demande[3]	1
Révisions judiciaires en cours en date du 31 décembre 2011 :	**25**
Requérant :	
Institutions	11
Auteurs de demande	3
Institutions et autres parties	4
Parties conçernées	7
Révisions judiciaires terminées ou entendues en 2011 :	**14**
Abandonnées (ordonnance ou décision du CIPVP maintenue)[4]	3
Ordonnance du CIPVP confirmée[5]	4
Ordonnance du CIPVP confirmée (appel en instance)[6]	1
Ordonnance du CIPVP confirmée en partie (appel en instance)[7]	2
Ordonnance infirmée; renvoi de l'affaire au CIPVP[8]	2
Intervention du CIPVP dans la demande[9]	2

1 2011 ONSC 7082
2 MO-2659
3 Règlement municipal de London
4 MO-2416 / MO-2449, MO-2489
5 MO-2425-I, MO-2521, PO-2739, PO-2807
6 PO-2811
7 PO-2872 / PO-2899-R
8 PO-2456, PO-2763
9 Ville de Toronto, Règlement municipal de London

Au tournant de l'année 2012, le CIPVP a entamé sa 25e année d'existence. J'ai parcouru tout un bout de chemin depuis mon arrivée au CIPVP à l'automne 1987, en tant que première directrice de l'application de la loi. J'ai le plaisir de travailler au CIPVP depuis 25 ans, et j'ai l'honneur d'occuper le poste de commissaire depuis 14 ans. Pendant cette période, il y a eu des changements considérables dans les domaines de l'accès à l'information et de la protection de la vie privée, celle-ci ayant évolué surtout à la suite des progrès sans précédent dans les technologies de l'information et des communications.

Tant de choses se sont passées depuis mon arrivée, de l'entrée en vigueur de la *Loi sur l'accès à l'information municipale et la protection de la vie privée* en 1990 à l'adoption de la *Loi sur la protection des renseignements personnels sur la santé* en 2004, sans compter l'adoption de la *protection de la vie privée intégrée* comme norme internationale. J'aurais tant à dire sur nos réalisations, mais nous ne pouvons aborder ici les milliers d'appels téléphoniques que le CIPVP reçoit chaque année, les nombreuses entrevues avec les médias, les travaux de recherche et d'élaboration de politiques, les enquêtes et appels sur la vie privée et les livres blancs, tout le travail associé à notre site Web, et plus encore. Je vous invite à visiter notre site Web à *www.ipc.on.ca*, car je crois que les résultats sont éloquents.

Le CIPVP entame sa 25e année au service de la population ontarienne, et l'avenir de l'accès à l'information et de la protection de la vie privée me préoccupe. Je crois toutefois que notre droit d'accéder à l'information que détient le gouvernement et notre droit à la vie privée demeureront protégés par ceux qui comprennent et apprécient le rôle que l'accès à l'information et la protection de la vie privée jouent dans une société libre et démocratique. Si nous vivions dans un monde idéal, un bureau comme le mien serait inutile, mais ce n'est pas le cas, et nous pouvons être reconnaissants à des gens tels que les membres de mon personnel et les milliers d'autres professionnels de l'accès à l'information et de la protection de la vie privée du monde entier pour leurs efforts constants en vue de protéger nos précieux droits.

Je suis persuadée qu'à l'avenir, l'un des plus grands obstacles à l'accès à l'information et à la protection de la vie privée représentera l'évolution toujours plus complexe de la technologie de l'information et des communications. Toutefois, la plus grande difficulté résidera non pas dans les progrès technologiques, mais dans l'apathie. Nous disposons des ressources et des outils nécessaires pour faire des progrès technologiques qui menacent l'accès à l'information et la protection de la vie privée des outils pour promouvoir ces valeurs, notamment grâce à la *protection de la vie privée intégrée* et à l'*accès à l'information intégré*. Pourtant, ces mesures n'auront de sens que si nous demeurons résolus à protéger ces droits.

Par conséquent, nous devons demeurer T***oujours vigilants***. Nous ne pouvons ménager nos efforts; nous devons mettre à profit les progrès réalisés et continuer de promouvoir le changement dans nos pays, territoires et organismes. Nous devons continuer de défendre les idéaux que sont l'accès à l'information et la protection de la vie privée. Nous ne pouvons nous asseoir sur nos lauriers et laisser nos droits, qui ont été si difficiles à obtenir, disparaître par manque de vigilance. Ce serait là une erreur fondamentale, qui établirait un précédent risquant d'aboutir au renversement de siècles de progrès sur le plan de la liberté. Le droit à l'information et à la protection de la vie privée est essentiel à la liberté. Comme disait Platon, philosophe de l'Antiquité, « l'un des préjudices d'avoir refusé de prendre part à la vie politique est que vous finissez par être gouverné par vos subordonnés ». Faisons en sorte que cela ne soit pas notre héritage.

Ann Cavoukian, Ph.D.

Commissaire à l'information et à la protection de la vie privée, Ontario, Canada

État financier

	Prévisions 2011-2012 $	Prévisions 2010-2011 $	Chiffres réels 2010-2011 $
Traitements et salaires	9 852 800	9 461 000	9 532 734
Avantages sociaux	2 266 600	2 176 200	1 768 832
Transports et communications	337 500	313 500	323 661
Services	2 052 300	1 890 800	1 827 516
Fournitures et matériel	239 000	194 000	316 223
Total	**14 948 200**	**14 035 500**	**13 768 966**

Remarque : L'exercice financier du CIPVP s'échelonne du 1er avril au 31 mars.
L'état financier du CIPVP est vérifié chaque année par le Bureau du vérificateur général de l'Ontario.

Droits d'appel perçus en 2011

(année civile)

Documents généraux	Renseignements personnels	Total
12 590 $	2 830 $	**15 420 $**

Voir autres renseignements financiers, y compris les traitements du CIPVP divulgués en vertu de la Loi de 1996 sur la divulgation des traitements dans le secteur public à www.ipc.on.ca

COMMISSAIRE À L'INFORMATION ET À LA PROTECTION DE LA VIE PRIVÉE DE L'ONTARIO
RAPPORT ANNUEL 2011

—

2, rue Bloor Est, Bureau 1400
Toronto (Ontario) M4W 1A8
Canada

Téléphone : (416) 326-3333
Télécopieur : (416) 325-9195
1-800-387-0073
ATS : (416) 325-9539

Courriel : info@ipc.on.ca
Site Web : www.ipc.on.ca